CLAIMS

1. (Currently Amended) A method for enciphering an information sequence for subsequent transmission comprising:

creating an original message by adding ~~one or more bits to said information sequence~~ a redundant bit to said information sequence at a most significant bit position;

comparing a numerical value of said original message to a predetermined value;

if the numerical value of said original message is equal to or greater than said predetermined value, changing at least one bit in said original message to obtain a modified message having a numerical value less than said predetermined value by changing said redundant bit at said most significant bit position; and

encrypting said modified message with a key associated with a first modulus.

2-3. (Cancelled).

4. (Original) The method of claim 1 wherein comparing a numerical value of said original message to a predetermined value comprises comparing said numerical value of said original message to said first modulus.

5. (Currently Amended) The method of claim 4 wherein changing at least one ~~redundant~~ bit in said original message to obtain a modified message having a numerical value less than said predetermined value further comprises changing at least one bit in said original message such that the numerical value of said modified message is less than said first modulus.

6. (Original) The method of claim 1 wherein creating an original message by adding one or more bits to said information sequence comprises adding one or more error detection bits to said information sequence.

7. (Original) The method of claim 6 wherein adding one or more error detection bits to said information sequence comprises computing a cyclic redundancy check code and appending said cyclic redundancy check code to said information sequence.

8. (Original) The method of claim 1 wherein encrypting said modified message with a key associated with a first modulus comprises encrypting said modified message with a private key based on said first modulus to obtain a signed modified message.

9. (Original) The method of claim 8 further comprising encrypting said signed modified message with a key associated with a second modulus less than said first modulus to obtain an encrypted modified message.

10. (Original) The method of claim 9 further comprising deciphering said encrypted modified message to obtain a first estimate of said modified message.

11. (Original) The method of claim 10 further comprising validating said first estimate of said modified message.

12. (Currently Amended) The method of claim 11 wherein validating said first estimate of said modified message comprises:

error decoding said first estimate of said modified message using ~~said~~ one or more error detection bits to generate an error indication;

if said error indication indicates no error, accepting said first estimate of said modified message as a reproduction of said original message;

if said error indication indicates an error, altering at least one predetermined bit in said first estimate of said modified message to obtain a modified estimate of said modified message; and

validating said modified estimate of said modified message.

13. (Original) The method of claim 12 wherein validating said modified estimate of said modified message comprises performing a bit alteration check to determine whether a predetermined bit of said modified message is an altered bit.

14. (Original) The method of claim 13 wherein performing a bit alteration check to determine whether a predetermined bit of said modified message is an altered bit comprises:

determining whether bit errors occurred in said at least one predetermined bit;

if bit errors occurred in said at least one predetermined bit, determining whether the value of said at least one predetermined bit has an expected value; and

if said at least one predetermined bit has an expected value, determining whether said modified estimate of said modified message has an expected value.

15. (Original) The method of claim 14 wherein determining whether bit errors occurred in said at least one predetermined bit comprises determining whether a bit error occurred in a most significant bit.

16. (Original) The method of claim 15 wherein determining whether the value of said at least one predetermined bit has an expected value comprises determining whether said most significant bit is equal to zero.

17. (Original) The method of claim 16 wherein determining whether said modified estimate of said modified message has an expected value comprises determining whether said modified estimate with said most significant bit position equal to one is greater than or equal to said encryption modulus.

18. (Currently Amended) A method of encrypting a message comprising the steps of:

forming an original message by appending one or more redundant bits to an information sequence;

comparing a value of said original message with a value of a first modulus and modifying said original message to obtain a modified message if said original message is greater than or equal to said first modulus;

signing said modified message with a first key based on said first modulus to form a signed message;

encrypting said signed message with a second key based on a second modulus to form a doubly encrypted message; ~~and~~

sending said doubly encrypted message to a recipient; and

wherein said original message has a length equal to said first modulus.

19. (Cancelled).

20. (Original) The method of claim 18 wherein signing said modified message with a first key based on said first modulus to form a signed message comprises signing said modified message with a sender's private key.

21. (Original) The method of claim 18 wherein modifying said original message to obtain a modified message if said original message is greater than or equal to said modulus comprises changing the value of one of said redundant bits.

22. (Original) The method of claim 18 wherein forming an original message by appending one or more redundant bits to an information sequence comprises adding error detection bits computed on said information sequence to said information sequence.

23. (Currently Amended) A method of deciphering a doubly encrypted bitstring comprising:

deciphering said doubly encrypted bitstring to obtain a once encrypted bitstring;

deciphering said once encrypted bitstring to obtain a first estimate of a plaintext message having one or more error detection bits;

decoding said first estimate of said plaintext message to produce ~~an~~ a first error indication;

if said first error indication indicates an error, performing a bit alteration check to determine whether a predetermined bit in said first estimate of said plaintext message was altered;

modifying said once encrypted bitstring if said bit alteration check produces an error by adding a predetermined value to said once encrypted bitstring, said predetermined value equal to a modulus associated with an encryption key used to generate said doubly encrypted bitstring;

deciphering said modified once encrypted bitstring to obtain a second estimate of said plaintext message;

decoding said second estimate of said plaintext message to produce a second error indication;

if said second error indication indicates an error, performing another bit alteration check to determine whether a predetermined bit in said second estimate of said plaintext message was altered.

24. (Original) The method of claim 23 wherein performing a bit alteration check to determine whether a predetermined bit in said first estimate of said plaintext message was altered comprises altering a predetermined bit in said first estimate of said plaintext message to generate a modified plaintext message and testing the validity of said modified plaintext message.

25. (Original) The method of claim 23 wherein performing a bit alteration check to determine whether a predetermined bit in said first estimate of said plaintext message was altered comprises checking said first estimate of said plaintext message for a bit error in a predetermined bit position.

26. (Original) The method of claim 25 wherein performing a bit alteration check to determine whether a predetermined bit in said first estimate of said plaintext message was altered further comprises determining a value of a bit in said predetermined bit position.

27. (Original) The method of claim 26 wherein performing a bit alteration check to determine whether a predetermined bit in said first estimate of said plaintext message was altered further comprises altering said value of said bit in said predetermined bit position to obtain a modified estimate of said plaintext message and comparing a value of said modified estimate of said plaintext message to a predetermined value.

28-30. (Cancelled).

31. (Original) A method of deciphering a doubly encrypted bitstring comprising:

deciphering said doubly encrypted bitstring to obtain a once encrypted bitstring;

modifying said once encrypted bitstring by adding an integer multiple of a modulus associated with an encryption key used to generate said doubly encrypted bitstring to said once encrypted bitstring to obtain a modified once-encrypted bitstring;

deciphering said modified once encrypted bitstring to obtain an estimate of said plaintext message.

32. (Original) The method of claim 31 further comprising decoding said estimate of said plaintext message to produce an error indication.

33. (Original) The method of claim 32 further comprising performing a bit alteration check to determine whether a predetermined bit in said estimate of said plaintext message is an altered bit, if said error indication indicates an error.

34-49. (Cancelled).